DOE CIO Guidance CS-15

U.S. Department of Energy

Cyber Security Program

PERSONALLY OWNED DEVICES GUIDANCE

January 2007

This Guidance document was developed and issued outside of the Departmental Directives Program.

1. PURPOSE.

   This Department of Energy (DOE) Chief Information Officer (CIO) Guidance provides establishes processes for the secure use of Personally Owned Devices for accessing, collecting, creating, processing, transmitting, disseminating, or storing DOE/Government information within and outside of DOE security areas.

   The DOE CIO will review this Guidance annually and update it as necessary. The DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) and their subordinate organizations and contractors (hereinafter called operating units) may provide feedback at any time for incorporation into the next scheduled update.

2. SCOPE.

   This Guidance provides additional information for Senior DOE Management for addressing the controls in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance,* and DOE Manual 205.1-4, *National Security Systems Controls Manual*, in their Program Cyber Security Plans (PCSPs). Specifically, this Guidance applies to computing devices that are personally owned.

3. CANCELLATIONS.

   None.

4. APPLICABILITY.

   a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to Which DOE CIO Guidance CS-15 is Applicable.*

      Further, Senior DOE Management may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their operating units, and for ensuring that those requirements are incorporated into contracts.

   b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.

c. DOE Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all systems collecting, creating, disseminating, accessing, processing, storing, or transmitting unclassified information. DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provide additional information for identifying unclassified information requiring protection.

d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security Systems. The protection mechanisms described in this guidance are consistent with and implement the policies and practices set forth by Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPOM);* the Atomic Energy Act of 1954, which established Restricted Data information; and EO 12958, *Classified National Security Information*, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides additional guidance for identifying National Security systems.

5. IMPLEMENTATION.

This Guidance is effective 30 days after issuance. However, DOE recognizes that this Guidance cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its issuance. If Senior DOE Management cannot address all of the criteria by that date, Senior DOE Management is to establish a Plan of Actions and Milestones (POA&M) for implementation of this Guidance into their PCSPs.

6. CRITERIA.

a. Senior DOE Management PCSPs are to define policies, processes, and procedures for the use of Personally Owned Devices with unclassified Federal information systems to include at least the following.

(1) Identification, documentation, and evaluation of business needs and circumstances under which use of Personally Owned Devices can be authorized for collecting, creating, disseminating, accessing, processing, storing, and transmitting DOE information.

(2) Documentation for the use of Personally Owned Devices in a System Security Plan (SSP).

(3) Policies for bringing Personally Owned Devices into areas where DOE unclassified information is being processed. These processes/procedures are to address:

(a) The controls used to reduce/eliminate the DOE TEMPEST/TSCM concerns (e.g. wireless, audio, video, infrared, etc.) when allowing the operation of these devices in security areas;

(b) The controls used to ensure that any connection of a Personally Owned Device to a Federal information system processing DOE information is made only if each system is accredited through processes that comply with DOE CIO Guidance CS-2, *Certification and Accreditation Guidance*; and

(c) Personnel training on the policies, processes, and procedures for the use of Personally Owned Devices and protection of Government information.

(4) Conditions for the use of Personally Owned Devices to process or store Sensitive Unclassified Information (SUI).

(5) Administrative procedures for enforcing the Senior DOE Management PCSP policy for the use of Personally Owned Devices, including actions to be taken when such devices are used in a manner inconsistent with the PCSP.

b. Program Cyber Security Plan. Senior DOE Management PCSPs are to comply with the criteria in DOE OCIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*, and DOE Manual 205.1-X, *National Security Systems Controls Manual*. Senior DOE Management PCSPs are to direct operating units to develop, document, and implement policies and procedures for Personally Owned Devices that comply with the following criteria and commensurate with the level of security required for the organization's environment and specific needs.

(1) The security controls for Personally Owned Devices are specified in an SSP, including software requirements, patching, virus protections, interconnections, etc.

(2) The SSP will address the use of Personally Owned Devices authorized to collect, create, disseminate, access, process, store, or transmit DOE/Government information, excluding information authorized for release to the public.

(a) The operational environment, protections, preferences, and settings for each device accessing Government networks and information are described in a SSP.

(b) The SSP must identify special restrictions and security considerations for use in areas outside of DOE security areas including at home or in transit/travel.

(3) Documented processes to ensure that Personally Owned Devices are connected to information systems processing DOE information only as allowed by the PCSP and SSP.

(4) The use of encryption capabilities conforming to CIO Guidance CS-38A, *Protection of Sensitive Unclassified Information, Including Personally Identifiable Information*, when transmitting to or from and storing Sensitive Unclassified Information on personally owned devices.

(5) Policies and procedures governing the mandatory collection of unauthorized Personally Owned Devices, including assessment, review, incident reporting, final disposition of the devices, and personnel actions when there is a potential incident.

(6) A process that provides for the reporting of security incidents including the theft or loss of Personally Owned Devices.

(7) Training and Awareness. The requirements for protecting Government information on Personally Owned Devices are to be reviewed with all users on a regular basis, at a minimum annually.

7. CRITERIA UNIQUE TO NATIONAL SECURITY SYSTEMS. Senior DOE Management PCSPs must define and document the following:

   a. Policies prohibiting the use of Personally Owned Devices in areas where classified data are discussed or processed.

   b. Policies prohibiting the use of Personally Owned Devices to access, collect, create, process, transmit, disseminate, or store classified information.

   c. Policies governing the mandatory collection and disposition of Personally Owned Devices that have been or are being used to access, collect, create, process, transmit, disseminate, or store classified information.

8. REFERENCES.

   DOE M 470.4-2, Change 1, *Physical Protection*, 08-26-05.

   Other references are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls*.

9. DEFINITIONS.

   Acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

DOE/Government Information. Information created, collected, processed, disseminated, or disposed, throughout its life cycle, by or on behalf of the DOE/ Federal Government.

Personally Owned Devices. Information systems, devices, media, or equipment owned by individuals and entities (e.g., businesses, colleges, etc) that are not included in a DOE SSP or controlled under a DOE PCSP. Personally Owned Devices include, but are not limited to, personal computers and related equipment, handheld and Personal Digital Assistant (PDA) devices, facsimile machines, photocopiers, enhanced cell phones, and storage devices such as flash memory (memory sticks), flash cards, portable hard drives, and MP3 players.

Portable/ Mobile devices. Portable and mobile devices are portable computing devices that provide the capability to collect, create, process, transmit, store, and disseminate information. These devices include (but are not limited to) laptop and notebook computers, mobile work stations, PDAs, enhanced cell phones, two way pagers, and wireless e-mail devices

10. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO GUIDANCE CS-15 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Health, Safety, and Security
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration